THE CLOUD HAS ITS BENEFITS IF THE RISKS ARE MANAGED WELL

The life sciences industry is a risk averse industry by nature. The way all our IT systems, applications and processes are regulated means we literally take good care of each and every step we take. And with good reason: whether it's direct or indirect, we want to reduce the risks for patient safety. But since times are changing our industry needs to change too, starting with our IT systems. Avoiding the cloud is no longer an option if we want to set up multiple supply chain channels, work together with third parties and want to start analysing big data.

Needless to say, one does not adopt a cloud strategy overnight. There are several risks involved when transitioning to the cloud and these need to be sorted out first. In this article we will look into the most important compliancy and security requirements your cloud provider should hedge when working with the life sciences industry.

COMPLY WITH INDUSTRY STANDARTS

Life sciences deal with very specific requirements with regards to quality and compliance. This means the choice of specialized and approved software applications or cloud solutions is limited. That doesn't mean your search for the right cloud strategy is over. On the contrary, there are specialized cloud platforms out there for you to consider or you can contact the cloud provider of your choice to discuss the possibilities of adjusting systems and processes to meet life science industry standards.

In general, a cloud provider should at least be prepared to secure your data and ensure an exquisite IT infrastructure:

- **Data backup and disaster recovery** - Make sure your data is protected, not only against cybercriminals but also against simple mistakes like misplacement or disposal accidents. Will the cloud provider execute a full backup? How often is data being backed up and where is it stored? And how can they help you when data needs to be recovered?

- **Audits** - To guarantee the quality of their IT infrastructure or software applications used, how often will the cloud provider undergo external audits (ISO or SOC)? Can they share the audit report with you? Certifications or guidelines such as GAMP, ITIL or ISO 27001, indicate IT systems are well maintained. In addition, documented evidence that systems work according to their intended purpose as outlined in Chapter 4 and Annex 11 of Eudralex, should be available and fully transparent to you.

THE CLOUD HAS ITS BENEFITS IF THE RISKS ARE MANAGED WELL

WHO CAN ACCESS SENSITIVE DATA

A comprehensive cloud strategy should consider that multiple persons have access to sensitive data. A cloud provider should be able to indicate who has access to your servers, systems and data. Sensitive data should not be accessible to just anyone, therefore it's important to understand the cloud provider's hiring process, service rotation schedules and access control procedures. Be certain to ask for the complete process for each data center your cloud provider works with. This gives you an insight in where your data is located and who can access it in any given point in time.

IN CHARGE OF SYSTEM UPDATES

The life sciences industry should be able to provide a system description document for any software application it works with regardless whether it's being managed on-premise or in the cloud. This should be a living document which shows the main system functionality, its regulatory impact, the system architecture and security features. Since a cloud application is managed by a third party, maintaining a system description becomes challenging. Discuss the purpose of such a document with your cloud provider and ask them to give notice prior to any system update. This way, together you can evaluate new (risk) consequences and either act in time or simply update your system descriptions.

REQUEST A SERVICE LEVEL AGREEMENT

As with any collaboration, it's important to discuss responsibilities before signing a contract. Who is responsible for maintaining your compliancy standards? Who should be in control of access management? Who holds actual encryption keys? What uptime do you agree on, who is responsible for actually maintaining the connectivity and what happens if this uptime isn't being met? A Service Level Agreement (SLA) should clarify the cloud provider's responsibilities with regards to maintaining system availability, data integrity and security.

AVAILABILITY

The availability of systems and data should be one of the main considerations when a cloud strategy is formulated. There are variances in uptime guarantees cloud providers offer and it's up to you whether an uptime of 99% will be enough, or if 99,99% uptime is a necessity? The difference between these percentages may seem trivial, but in effect it means a total allowance of annual downtime of 3,6 days compared to less than an hour. The right cloud provider will be able to guarantee uptimes which are tailored to the needs of the life sciences industry.

ADOPTING THE CLOUD FOR LIFE SCIENCES

In this series of articles, we will take a closer look at the advantages cloud solutions hosted in data centers have to offer life sciences in comparison to on premise IT-infrastructures. Since risk management is a main priority when handling medical digital data, we will first take a look at what constitutes the cloud and which criteria should be met when considering adopting cloud solutions for life sciences. From there we will tackle (growing) concerns about cybersecurity, based on awareness and the 'four eyes' approach. Finally, we will examine why excellent connectivity is the foundation of the life sciences in the twenty-first century and how opting for the cloud ensures that connections are always available.